**Fortinet dołącza do inicjatywy Komisji Europejskiej Cybersecurity Skills Academy**

*Podążając za znajdującą się w misji firmy deklaracją, jaką jest likwidowanie luki w cyfrowych kwalifikacjach na całym świecie, Fortinet zadeklarował uczestnictwo w działaniach Unii Europejskiej mających na celu wzrost wiedzy oraz przekwalifikowywanie się jej obywateli.*

**[Warszawa, 25.03.2024] Fortinet, globalny lider cyberbezpieczeństwa, który dąży do konwergencji sieci i rozwiązań ochronnych, dołączył do rozpoczętej przez Komisję Europejską** [**inicjatywy**](https://digital-skills-jobs.europa.eu/en/inspiration/pledges/fortinet-cybersecurity-skills-academy-pledge)[**Cybersecurity Skills Academy**](https://digital-skills-jobs.europa.eu/en)**. Za pośrednictwem działu** [**Fortinet Training Institute**](https://www.fortinet.com/nse-training)**, Fortinet** [**zobowiązał się**](https://digital-skills-jobs.europa.eu/en/inspiration/pledges/fortinet-cybersecurity-skills-academy-pledge) **zaoferować bezpłatnie swoje wielokrotnie nagradzane szkolenia z zakresu cyberbezpieczeństwa oraz program podnoszenia świadomości w zakresie bezpieczeństwa nawet 75 tys. osobom w Europie w ciągu najbliższych trzech lat. Zobowiązanie to ma na celu zmniejszenie niedoboru umiejętności w zakresie cyberbezpieczeństwa w całej Unii Europejskiej (UE), przyczyniając się dodatkowo do realizacji globalnego celu Fortinet wyznaczonego w 2021 r., jakim jest przeszkolenie miliona osób na całym świecie w zakresie cyberbezpieczeństwa w ciągu pięciu lat.**

**Rozwój unijnej siły roboczej w dziedzinie cyberbezpieczeństwa w celu zwiększenia odporności regionu**

Taktyki przyjmowane przez cyberprzestępców stają się coraz bardziej wyrafinowane, dzięki czemu szybko identyfikują oni sposoby na uniknięcie kontroli bezpieczeństwa. Mimo to wielu liderów biznesu nie dysponuje personelem odpowiedzialnym za bezpieczeństwo, który jest niezbędny do odpowiedniej ochrony firmowej sieci. Około 40% decydentów IT w UE uważa, że rekrutacja, zatrudnienie i utrzymanie wykwalifikowanych specjalistów ds. bezpieczeństwa [stanowi wyzwanie](https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf), a prawie 50% twierdzi, że trudno jest osiągnąć cele w zakresie różnorodności, takie jak zatrudnianie większej liczby kobiet, weteranów wojskowych i osób pochodzących z mniejszości.

Zadaniem uruchomionej przez Komisję Europejską w 2023 r. inicjatywy [Cybersecurity Skills Academy](https://digital-skills-jobs.europa.eu/en/latest/news/closing-cybersecurity-talent-gap-commission-launches-cybersecurity-skills-academy) jest pomoc w likwidowaniu luki w umiejętnościach w zakresie cyberbezpieczeństwa w UE poprzez współpracę prywatnych i publicznych podmiotów w celu promowania wiedzy w zakresie cyberbezpieczeństwa i rozwoju siły roboczej. Akademia stanowi wspólny punkt dla osób fizycznych, instytucji akademickich i przedsiębiorstw, którzy zyskują dostęp do szkoleń, certyfikatów i możliwości finansowania w zakresie cyberbezpieczeństwa.

Dołączając do tej ważnej inicjatywy Fortinet będzie oferować [program certyfikacji](https://www.fortinet.com/training-certification?utm_source=pr&utm_medium=pr&utm_campaign=training-certification) Fortinet Training Institute za pośrednictwem Cybersecurity Skills Academy, aby jeszcze bardziej zwiększyć dostęp do szkoleń w zakresie świadomości cyfrowej ochrony i przyczynić się do rozwijania niezbędnych umiejętności oraz pomagania osobom w rozwoju kariery w dziedzinie bezpieczeństwa lub rozpoczęciu pracy w tej branży.

**Zaangażowanie Fortinet w likwidację globalnej luki w umiejętnościach w zakresie cyberbezpieczeństwa**

Zaangażowanie firmy Fortinet w prowadzoną przez Komisję Europejską inicjatywę Cybersecurity Skills Academy jest odzwierciedleniem jej wieloletniego zaangażowania w likwidację luki w umiejętnościach w zakresie cyberbezpieczeństwa na całym świecie.

Dział [Fortinet Training Institute](https://www.fortinet.com/nse-training) służy specjalistom ds. IT i bezpieczeństwa, studentom oraz nauczycielom, a także społecznościom poszukującym dodatkowych kwalifikacji, w tym kobietom i weteranom, poprzez różne programy, takie jak [Academic Partner](https://www.fortinet.com/training/academic-partner-program?utm_source=pr&utm_medium=pr&utm_campaign=academic-partner-program) oraz [Education Outreach](https://www.fortinet.com/training/education-outreach-program?utm_source=pr&utm_medium=pr&utm_campaign=education-outreach-program).

**Rob Rashotte, Vice President of Global Training and Global Field Enablement, Fortinet**

Fortinet zobowiązał się do powszechnego udostępniania materiałów edukacyjnych i szkoleń w zakresie cyberbezpieczeństwa, aby zaradzić globalnemu niedoborowi talentów. Kluczową rolę w tych wysiłkach odgrywają partnerstwa publiczno-prywatne. Dlatego współpraca w ramach organizowanej przez Komisję Europejską inicjatywy Cybersecurity Skills Academy jest zgodna z naszym celem, jakim jest zapewnienie szkoleń w zakresie cyberbezpieczeństwa dla miliona osób na całym świecie do 2026 roku. Z niecierpliwością czekamy na zwiększenie zakresu możliwości uczenia się osobom we wszystkich 27 krajach Unii Europejskiej w celu rozwoju cyberprzestrzeni w regionie.

**Dodatkowe zasoby**

* Więcej informacji o organizowanych przez Fortinet [darmowych szkoleniach dotyczących cyberbezpieczeństwa](https://www.fortinet.com/training/cybersecurity-professionals?utm_source=blog&utm_campaign=freetraining), obejmujących szeroki zakres informacji produktowych oraz budujących świadomość dotyczącą cyberzagrożeń. Jako część składowa strategii Fortinet Training Advancement Agenda (TAA), Fortinet Training Institute prowadzi także szkolenia i certyfikacje w ramach programów [Network Security Expert (NSE) Certification](https://www.fortinet.com/training-certification), [Academic Partner](https://www.fortinet.com/training/security-academy-program) oraz [Education Outreach](https://www.fortinet.com/training/education-outreach-program).
* Więcej informacji o prowadzących badania nad zagrożeniami oraz publikujących raporty [Outbreak Alert](https://www.fortinet.com/fortiguard/outbreak-alert?utm_source=pr&utm_campaign=outbreak-alert) laboratoriach [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=FortiGuardLabs), które zapewniają podjęcie w odpowiednim czasie działań mających na celu złagodzenie skutków cyberataków.
* Więcej informacji o [portfolio](https://www.fortinet.com/solutions/enterprise-midsize-business/security-as-a-service/fortiguard-subscriptions) usług bezpieczeństwa świadczonych przez należący do Fortinet dział FortiGuard.
* Przeczytaj w jaki sposób [klienci Fortinet](https://www.fortinet.com/customers?utm_source=website&utm_medium=pr&utm_campaign=customers) zabezpieczają swoje przedsiębiorstwa.
* Profile firmy Fortinet w mediach społecznościowych: [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet), [Facebook](https://www.facebook.com/fortinet/), [YouTube](https://www.youtube.com/channel/UCJHo4AuVomwMRzgkA5DQEOA?sub_confirmation=1) oraz [Instagram](https://www.instagram.com/behindthefirewall/).

**Informacja o firmie Fortinet**

Firma Fortinet jest czołowym producentem systemów ochronnych i innowatorem przyczyniającym się do ich ewolucji, co umożliwiło stworzenie rozwiązań zapewniających konwergencję funkcji sieciowych i zabezpieczających środowisko IT. Jej misją jest ochrona ludzi, urządzeń i danych, niezależnie od ich miejsca. Obecnie producent zapewnia cyberbezpieczeństwo wszędzie tam, gdzie potrzebują go klienci, dzięki największemu portfolio ponad 50 zintegrowanych ze sobą produktów klasy korporacyjnej. Znacznie ponad pół miliona klientów zaufało rozwiązaniom Fortinet, które należą do najczęściej wdrażanych, posiadających najwięcej patentów i najlepiej ocenianych w branży. Instytut szkoleniowy Fortinet (Fortinet Training Institute), jeden z największych i najszerszych programów szkoleniowych wśród dostawców rozwiązań ochronnych, gwarantuje, że szkolenia z zakresu cyberbezpieczeństwa oraz nowe możliwości rozwoju kariery są dostępne dla każdego. Natomiast FortiGuard Labs to elitarny oddział firmy Fortinet, który zajmuje się badaniem i analizą zagrożeń, opracowuje i wykorzystuje wiodące mechanizmy uczenia maszynowego oraz sztucznej inteligencji, aby zapewnić klientom terminową, nieustannie najlepszą ochronę i dostęp do informacji o zagrożeniach. Więcej informacji dostępnych jest na stronie [https://www.fortinet.com](https://www.fortinet.com/), blogu Fortinet oraz stronie FortiGuard Labs.

**Copyright © 2023 Fortinet, Inc**. Wszelkie prawa zastrzeżone. Symbole ® oraz ™ oznaczają odpowiednio zarejestrowane federalnie znaki towarowe i znaki towarowe prawa zwyczajowego firmy Fortinet, Inc. oraz jej podmiotów zależnych i stowarzyszonych. Znaki towarowe firmy Fortinet obejmują, ale nie ograniczają się do następujących: Fortinet, logo Fortinet, FortiGate, FortiOS, FortiGuard, FortiCare, FortiAnalyzer, FortiManager, FortiASIC, FortiClient, FortiCloud, FortiMail, FortiSandbox, FortiADC, FortiAI, FortiAIOps, FortiAntenna, FortiAP, FortiAPCam, FortiAuthenticator, FortiCache, FortiCall, FortiCam, FortiCamera, FortiCarrier, FortiCASB, FortiCentral, FortiCNP, FortiConnect, FortiController, FortiConverter, FortiCWP, FortiDAST, FortiDB, FortiDDoS, FortiDeceptor, FortiDeploy, FortiDevSec, FortiEDR, FortiExplorer, FortiExtender, FortiFirewall, FortiFone, FortiGSLB, FortiGuest, FortiHypervisor, FortiInsight, FortiIsolator, FortiLAN, FortiLink, FortiMonitor, FortiNAC, FortiNDR, FortiPAM, FortiPenTest, FortiPhish, FortiPolicy, FortiPortal, FortiPresence, FortiProxy, FortiRecon, FortiRecorder, FortiSASE, FortiSDNConnector, FortiSIEM, FortiSMS, FortiSOAR, FortiSwitch, FortiTester, FortiToken, FortiTrust, FortiVoice, FortiWAN, FortiWeb, FortiWiFi, FortiWLC, FortiWLM i FortiXDR. Inne znaki towarowe należą do ich właścicieli. Firma Fortinet nie zweryfikowała w niezależny sposób oświadczeń lub certyfikatów przypisywanych osobom trzecim w niniejszym dokumencie, a także nie udziela niezależnego poparcia takim oświadczeniom. Niezależnie od wszelkich postanowień zawartych w niniejszym dokumencie, żaden z jego zapisów nie stanowi gwarancji, rękojmi, umowy, wiążącej specyfikacji ani innego wiążącego zobowiązania firmy Fortinet, ani też nie wskazuje na intencje związane z wiążącym zobowiązaniem, a wydajność i inne informacje o specyfikacji zawarte w niniejszym dokumencie mogą być unikalne dla niektórych środowisk.